USAWC STRATEGY RESEARCH PROJECT

DEVELOPING JOINT INFORMATION OPERATIONS WARRIORS

by

Lieutenant Colonel James A. Pickle
United States Air Force

Colonel David J. Smith
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **15 MAR 2006**	2. REPORT TYPE	3. DATES COVERED

4. TITLE AND SUBTITLE **Developing Joint Information Operations Warriors**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **James Pickle**	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**22**	

ABSTRACT

AUTHOR:	Lieutenant Colonel James A. Pickle
TITLE:	Developing Joint Information Operations Warriors
FORMAT:	Strategy Research Project
DATE:	13 April 2006 WORD COUNT: 6,098 PAGES: 21
KEY TERMS:	IO, influence, PSYOP, electronic warfare, computer network operations, public affairs
CLASSIFICATION:	Unclassified

The Department of Defense (DoD) has recognized the importance of information operations (IO), particularly in light of continual technological improvements. Positive direction has been given by the Office of the Secretary of Defense and the Joint Staff but the responsibility to organize, train, and equip remains with the Services and allows for different interpretations. The goal of IO is to maintain information superiority and thereby decision superiority. While influence operations may aim at adversary perceptions, joint IO can’t be left open for interpretation. Information is impacting the spectrum of conflict more than ever before. Information dominance has always been important but the speed and methods at which it can be sent, analyzed, and acted upon is increasing exponentially. This project focuses on the need for a dedicated IO career force for the DoD to truly achieve information dominance. The analysis begins with a quick review of joint IO doctrine, Service approaches to IO, and IO personnel management. Next IO education and training challenges are explored. Finally, recommendations to improve joint IO are broached in an effort to ensure DoD IO warriors can influence, disrupt, degrade, or deny an adversaries ability to make a coherent decision at a time of our choosing.

DEVELOPING JOINT INFORMATION OPERATIONS WARRIORS

Sun Tzu might be considered the very first Information Operations (IO) warrior even if he didn't call it IO. He understood the importance of deception, of an integrated military strategy, and of a coherent message to his adversary. "To subdue the enemy without fighting is the acme of skill."[1] IO isn't new, what is relatively new is the formal Department of Defense (DoD) direction of IO as a core military competency. The new Joint Publication (JP) 3-13, *Information Operations*, states "IO are integral to the successful execution of military operations." Around the world "across a range of unusual battle-spaces – global computer networks, human psychology, and electronic systems"[2] the DoD is engaged in IO. This new focus is driven by the technological developments that allow information to be shared across distances, languages, and barriers inconceivable only a few years ago.

DoD is moving forward. In the last three years the following policy and doctrine documents have been published or updated:

- Classified *Information Operations Roadmap* – Oct 03*;*
- *Defense Planning Guidance (DPG) 04-09*;
- DoD Directive 5143.01, *Undersecretary of Defense for Intelligence (USD(I))* – Nov 05*;*
- DoD Instructions (DoDI) 3608.11, *Information Operations Career Force* – Nov 05*;*
- DoDI 3608.12, *Joint Information Operations Education* – Nov 05;
- JP 3-13, *Information Operations* – Feb 06*;*
- *Quadrennial Defense Review* – Feb 06*;*

These documents lay a joint doctrinal foundation for the DoD IO career field and designate the USD(I) as the functional proponent, responsible for policy and oversight, of the IO career force.[3]

Dedicated IO professionals are essential for DoD IO to provide information dominance. Beginning "with the end in mind,"[4] how should the DoD grow a chief IO officer, such as the Deputy Director for Global Operations (J-39), for the Joint Staff or U.S. Strategic Command (USSTRATCOM)? No adequate guidance currently exists. This research suggests to attain the full promise of DoD IO, a joint-level approach to train IO warriors is needed. To understand the problem of creating joint IO, one must first examine the background of current IO doctrine and the Services approach to IO. DoDI 3608.11 and 12 establish the requirement to train an IO career force comprised of IO capability specialists and IO planners. But there are multiple challenges to meeting the USD(I) guidance. Finally, having considered the dilemma, this analysis offers a few recommendations to get the most from limited funding and allow the creation of a true joint IO warrior.

Laying the Information Operations Doctrinal Foundation

DPG 04-09 directed each service to develop an IO career force. The *IO Roadmap* provided amplifying guidance. DoDI 3608.11 directs "an IO Career Force shall be established and maintained to plan and execute fully integrated IO."[5] DoDI 3608.11 further defines two categories within the IO career force for both the Active and Reserve component: IO capability specialists and IO planners. An IO capability specialist is "a functional expert in one or more of the specialized core capabilities."[6] An IO planner is "a functional expert trained and qualified to plan and execute full spectrum IO."[7] The instruction further directs education, training, and experience standards be established and requires an annual update to the Secretary of Defense (SecDef). The goal is to provide a DoD-wide, common foundation of IO knowledge and proficiency.[8]

DoDI 3608.12 establishes a Board of Advisers (BoA) and a BoA working group for joint IO education with the Joint Staff and USSTRATCOM each providing a general officer as a co-chair for the BoA. Joint Forces Staff College is tasked to develop and conduct a joint IO planner course. The Naval Post Graduate School is tasked to establish an IO Center of Excellence and a graduate level joint IO education program.[9] Though newly formed, the BoA working group has already met twice and the BoA once. The DoDIs provide the USD(I) intent for joint IO career force and education but not program specifics. Specific educational requirements are left to the BoA and the individual services.

The new JP 3-13 IO definition identifies five core IO capabilities. IO is "the integrated employment of the core capabilities of electronic warfare [EW], computer network operations [CNO], psychological operations [PSYOPS], military deception [MILDEC], and operations security [OPSEC], in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decisionmaking while protecting our own."[10] Along with the five core capabilities, JP 3-13 also identifies five supporting capabilities: information assurance (IA), physical security, physical attack, counterintelligence, and combat camera. Supporting capabilities either directly or indirectly contribute to full spectrum IO. Also three other military functions are related capabilities for IO: public affairs (PA), civil military operations (CMO), and defense support to public diplomacy. "These capabilities make significant contributions to IO and must always be coordinated and integrated with the core and supporting IO capabilities. However, their primary purpose and rules under which they operate must not be compromised by IO." [11] Of note, the new JP 3-13 removes information warfare as a term from joint doctrine and discontinues us of the terms offensive and defensive IO but retains that IO is applied to achieve both offensive and defensive objectives.[12]

What is the principal goal of IO? - "To achieve and maintain information superiority for the US and its allies."[13] Information superiority enables decision superiority. Decision superiority allows our forces to observe, orient, decide, and act faster than our adversaries. To train IO warriors one must understand the battlefield. For IO that battle-space is the information environment. IO gains information superiority is by taking control of the information environment. "The information environment is where humans and automated systems observe, orient, decide, and act upon information, and is therefore the principle environment of decisionmaking."[14] The information environment is comprised of "three interrelated dimensions: physical, information, and cognitive."[15] The physical dimension is the easiest to measure and the dimension combat power is traditionally applied. The information dimension consists of the content and flow of information and it must be protected. The cognitive dimension is the most important of the three dimensions. It encompasses the mind of the target audience (TA). It is the dimension of perception and eventual decisions.[16] IO impacts the decisionmaker by taking actions to add, modify, or remove information from an individual's environment, by affecting the infrastructure that supports the decisionmaker, or by influencing the way people receive, process, and use data and information.[17] Specific methods to influence a TA require focused training.

IO Core Capabilities

Each of the five IO core, supporting, and related capabilities have existed long enough that most of their doctrine, Service and joint training is established, understood, and used. Several of the capabilities have been practiced for centuries. In the modern age with the U.S. emphasis on information superiority, EW and CNO have been developed and added to these legacy capabilities. A short discussion of each of the core capabilities helps in comprehending some of the challenges for a joint IO career force.

"PSYOP has a central role in the execution of IO at all levels … As the information environment evolves the delivery means … are expanding from traditional print and broadcast … to internet, facsimile, text messaging, and other emerging media." [18] More than any other IO core capability, PSYOP requires cultural understanding and language training. PSYOP is a direct accession within the Army. Officers are trained and retained as PSYOP professionals.

The other Services and U.S. Special Operations Command (USSOCOM) use the Army PSYOP school to train their personnel.

MILDEC are "those actions executed to deliberately mislead adversary decisionmakers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that"[19] contribute to the friendly mission accomplishment. MILDEC exploits the adversary's information systems, processes, and capabilities, and like PSYOP, is fundamental to IO. MILDEC requires formal training. However, once trained, individuals may or may not serve in a deception position again. By the nature of the program, these operations are normally hidden from the broad military population.

OPSEC is the process of identifying essential elements of friendly information that could be gathered by adversaries to create an accurate picture of our forces, capabilities, and intentions and then denying that information to them. It is not a career field in any of the Services. OPSEC is a formal program, requiring annual training for all personnel, and a designated program manager. Training is normally computer based and individually paced. Physical security, IA, and computer network defense must complement OPSEC for it to be effective.

EW includes three subdivisions: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). "EW contributes to the success of IO by using maneuver, attack, and defense in a variety of combinations to shape, disrupt, and exploit adversarial use of the electromagnetic spectrum while protecting friendly freedom of action in that spectrum."[20] EW core specialists perform a dynamic role during combat planning ensuring constant deconfliction between the dilemma of exploitation versus denial. EW training serves as a model for joint IO training since Navy, Air Force, and Marine EW aviators all receive their basic EW training at Pensacola. For the AF that EW training follows initial navigator training since AF electronic warfare officers are navigators. Additionally, the EA-6B is a joint EW platform utilizing all three services as mission crew. The Army is developing their EW program at three locations: EA at Ft Sill along with effects based operations in the fire and effects coordination cell, EP at Ft Knox, and ES at Ft Huachuca.

CNO is comprised of computer network attack, computer network defense, and computer network exploitation. Our world had come to depend upon technological networks for our very existence; power grids, highways, water distribution, and information networks. "As the capability of computers and the range of their employment broadens, new vulnerabilities and opportunities will continue to develop … both to attack and exploit and adversary's computer system … [and] to identify and protect our own from similar attack and exploitation."[21] Currently there isn't a joint doctrine for CNO. The Joint Task Force for Global Network Operations (JTF-GNO) under USSTRATCOM is developing standard operating and reporting procedures. But JTF-GNO has no punitive authority to enforce standards and reporting procedures.

This paper focuses on joint IO training, but any discussion on joint training requires an overview of each of the Services respective IO doctrine and approach to IO training since the Services are tasked to organize, train, and equip.

Service approach to IO

Army

The Army has embraced the development of an IO career force with the creation of IO career field (IOCF) including seven functional areas (FA). These FAs include Information Systems (IS) Engineering, IS Management, Strategic Intelligence, Public Affairs, Space Operations, Simulation Operations, and Information Operations. The Information Operations (FA 30) is the integrating FA. Even though the Army recognizes the same core, supporting, and related IO capabilities from joint doctrine, PSYOP and EW are not included in the Army IOCF! Army officers are designated into the IO FA between their 5th and 6th years of service. The FA 30 IO training is 3 months long. Minimally, officers will not begin FA 30 training until they have qualified for captain in their basic branch. Many will not serve in a FA 30 assignment until selected for major and placed in the IOCF by a Career Field Designation Board. Only initial IO training is identified in the career path. The remainder of an Army IO career is comprised of IO assignments at increasing levels of responsibility starting at the maneuver brigade, then division through joint staff and normal professional military education (PME) unless an individual is selected to attend a civilian university instead of PME. The concept is to expose the officer to a variety of IO environments.[22] The Army is farther ahead with the establishment of an IOCF, but it doesn't provide for direct accessions as an FA 30.

Air Force

The Air Force (AF) believes that IO are integral to all AF operations. Air Force Doctrine Document 2-5, *Information Operations*, identifies three IO capabilities – influence operations, EW operations, and network warfare operations. Within influence operations they group the military activities of PSYOP, MILDEC, OPSEC, counterintelligence, counterpropaganda, and PA with the caveat "while a component of influence operations, (PA) is predicated on its ability to project truthful information to a variety of audiences."[23] Network warfare is broken into network attack, network defense, and network warfare support similar to CNO. EW is the same as joint doctrine.

The AF IO career force approach is slightly different also. Rather than an AF IO career field, the AF will create an IO career force from 19 existing career fields within the AF. Once trained in IO, the officer’s AF Specialty Code includes a special experience identifier (SEI) so they may be tracked in the AF personnel system. These 19 career fields include related capability fields as electronic warfare officers (navigators), public affairs, communications, along with combat operations fields as pilots and air battle managers, as well as legal, behavioral science, scientists, and the office of special investigations to name a few. Each of these officers would retain their primary career field with an SEI to highlight their IO experience. The closest major weapons system associated with IO, from the AF perspective, is the Aerospace Operations Center (AOC). Air Combat Command (ACC) has been given the major command lead for IO. Air Education and Training command is evaluating IO courseware through a formal course development process. The current course is six weeks long. One difficulty for the AF is that without a career field there isn’t an air staff flag officer advocate for funding and other doctrine, training, and organization issues. An IO general officer steering group is reviewing this issue. As ACC works the AF IO mission essential task list there is a major effort to balance resources while providing a minimum IO training competency. [24]

Navy

The Navy doctrine recognizes the same core capabilities as joint doctrine. The Navy is in mid stride in developing IO warriors. In 1994, the Commander, Naval Security Group, was designated as the Executive Agent for IW/C2. In 2005, they converted all their officer “cryptologists” to "information warfare" following IO direction in the DPG 04-06 and the DoD IO Roadmap. The Navy has significant capabilities in EW and CNO compared to lesser capabilities in OPSEC and MILDEC. The Navy is working on a job task analysis of determining which positions should be manned by what type of IO career officer and what training they will need to succeed at the respective level. Aside from core capability area training in traditional SIGINT and EW disciplines, the beginning course for planners is an IO staff officer course of 2 weeks duration, taught in fleet concentration areas. Time and funding permitting, they attempt to utilize the courses available at Joint Forces Staff College (JFSC). The Navy has a unique IO challenge due to their funding lines. Major program funding is tied to platforms. There is no dedicated single IO resource sponsor to sponsor investment that is not unique to a submarine, aircraft or surface vessel. In the terms of EW technology, the Navy is building new architectures which can be used across multiple major programs with only minor software modifications to ensure EW and IO integration. Most dedicated IO expertise is found in the IW officer community and cryptologic technician enlisted community. Officers and enlisted personnel from more traditional warfare areas (aviation, surface, and subsurface communities) can be assigned to IO billets, either in a capability area or as an IO planner, but these communities do not normally count themselves as part of the IO Career Force. The major exception to this would be the EA-6B (Prowler) community which counts EW as their primary mission area and therefore, a member of the IO Career Force. While IO planners may come from unrestricted line officers (URL), these officers normally only serve one tour in the IO community. While a URL officer has the combat focus they may not have an IO skill set or expertise. The Navy concept is to use IO capability specialists in IO planner positions vice creation of a new IO "generalist" career field.[25]

Marines

While the Marines have IO officer military occupational specialties (MOS), they take a slightly different view with regard to IO:

> IO is not simply another arrow in the MAGTF [Marine Air-Ground Task Force] commander's quiver, but is a broad-based integrative approach that makes the bow stronger. This distinction is key to our belief that IO does not, and will not, replace any of the time-tested warfighting functions, rather, it will enable each of them. Thus, the focus of Marine Corps IO will be upon the information-oriented activities that will best support the tailored application of combat power and the joint force commander's needs.[26]

The Marines have a robust cadre of electronic warfare officers. A small number have graduated from the NPS with a master's degree in Information Warfare. These officers were initially designated an information warfare officer MOS, the MOS name changed to an IO officer, and finally a Technical IO officer (MOS 9634) in 2005 to reflect the changes in the NPS course.[27] The IO Technical officers are used in positions requiring a technical background (requirements, plans, and policies). Additionally, the Marines have an IO Staff officer (MOS 9934) created in 2004 in response to the DPG direction to create an IO career force and is used to designate an IO officer serving on a MAGTF staff or another staff. The 9934 is an "additional" MOS, as officers in this MOS continue to serve in their primary MOS with periodic tours in IO. These officers must complete a course of study at least two weeks in length to include the Navy, JFSC, or the Army school at Ft Belvoir and serve a minimum of 6 months in an IO billet performing IO duties. The IO Technical officer and IO Staff officer are IO planners. The Marine capability specialists are defined through their area of expertise, such as an EA-6B pilot, CNO, or PSYOP. The Marines are also adding two new MOSs for company grade and enlisted IO personnel to better track IO experience and expertise.[28]

In summary, all of the Services are working diligently on their respective IO career force. Each is a constantly moving target with constant changes to optimize IO for their service. None of the Services have direct accession into the IO planner career field. There are direct accessions into some of core capabilities but not IO planners. However, it is the IO planners who are expected to lead the IO cells around the world within the combatant commands. IO planners should have a technical IO background to fully understand IO execution and integration. If IO is a core military competency, shouldn't an IO planner be a direct accession into the IO career field? The problem stems from their there being too little IO history and too much specific capability history. With the DoD direction to establish an IO career force, the Services have merged several independent but related activities. Each of those core capabilities brings some inherent baggage and inertia with them. The IO "ores" have been smelted but an IO alloy hasn't bonded. It might have taken less time to start from a clean slate, but the military could not afford to lose the history, skill, experience, and knowledge in the core capabilities.

Discussion

The civilian leadership has thrown the gauntlet. "The QDR identified capability gaps in each of the primary supporting capabilities of … Information Operations … to close those gaps, the Department will focus on organizing, training, equipping, and resourcing the key communication capabilities. This effort will include developing new tools and processes for assessing, analyzing, and delivering information to key audiences as well as improving linguistic and cultural competence … with the goal of achieving a seamless communication across the U.S. Government."[29] JP3-13 states, "The development of IO as a core military competency and critical component to joint operations requires specific expertise and capabilities at all levels of DoD… At each level of command, a solid foundation of education and training is essential to the development of a core competency."[30] It's a Catch-22 situation. "Professional education and training, in turn, are dependent on the accumulation, documentation, and validation of experience gained in operations, exercises, and experimentation."[31]

JP 3-13 identifies three basic tenets of IO education and training: the IO career force should consist of both core capability specialists (EW, PSYOP, and CNO) and IO planners, Initial capability specialist training and education requirements are Service and capability specific, and IO planners are required at both the component and joint level. Joint IO training directs joint doctrine and policies and assumes a solid foundation of Service-level IO training.[32] But that hasn't happened yet. "Within DoD, over 400 IO-related courses currently provide knowledge and skill training to IO planners and capability specialists. Some…are redundant. There is neither a formal DoD-wide standard on how IO knowledge and skills are trained, nor a single formal plan to ensure that information presented by different organizations for similar course objectives are standardized."[33] While the new JP 3-13 and DoDIs now provide joint IO doctrine, many of the current courses are service specific and were developed without any formal process to ensure the objectives and content were consistent. Additionally, since the courses aren't standardized there is some rivalry with regard to curriculum. The previous lack of joint doctrine and still developing Service doctrine contributes to constantly evolving IO tactics, techniques, and procedures (TTPs). This wastes limited funds for the IO community with redundant courses, instructors, and materials. It breeds a lack of confidence in the general military population because of differing knowledge and skill levels and different TTPs for implementing IO. This lack of confidence impacts leaders and their willingness to release personnel for initial or advanced training. Previous IO courses were cancelled because commanders were unwilling to pay for or to allow personnel to attend courses exceeding three weeks. Additionally, the inconsistency makes IO a harder "sell" for future IO career force recruits. Now that USD(I) has directed IO become a core competency, Service doctrine should solidify and align with Joint doctrine.

The Services are responsible for career training for their IO career force and general populations based upon identified joint force mission requirements. Service-wide training of military personnel should account for the nature of the information environment and that individual actions can affect the view of foreign populations.[34] IO impacts perceptions and positive perceptions can be destroyed in an instant by an adversary or the local media if given the opportunity by an inadvertent cultural *faux pas* or outright criminal act by any member of the military. The SecDef and the Services have realized how critical language and cultural skills are to IO. This is reflected in the QDR and in the Services push for increased language training outside that already utilized in the intelligence community. "Misperception and misunderstanding are complicated and reinforced when joint forces do not have sufficient language and cultural skills to communicate effectively with the populations among whom they operate."[35]

One of the greatest challenges for IO is the education IO warriors need to learn how to think about IO:

> IO requires very detailed analysis and skilled synthesis, fueled by specific subject matter expertise and knowledge. IO requires its practitioners to synthesize and to view problems and challenges as holistic and related instead of isolated. Each part of IO relates to other parts just as actions in one part of the world in one domain can cascade into other parts of the world and in other domains. IO education must give people a broad appreciation of how different cultures affect how people think, plan, and interpret outcomes. IO planners also need education sufficient for conducting sophisticated wargaming going back and forth from the mind of the friendly commander to the mind of other participants in conflict who have influence on friendly COAs.[36]

IO warriors must be able to detect patterns and opportunities within the information environment. This requires increasingly in-depth instruction appropriate to the leadership level. Such training requires a solid foundation and continual education reinforced and enhanced throughout a career. What strategy should be reinforced in the curriculum, IO as influence and technical, offensive and defensive, denial and exploitation, or lethal and non-lethal? All must be addressed.

Not only is the standardization of current knowledge an issue for IO; another challenge, in particular for CNO, is the pace of technology and related education. Moore's law states computing power doubles every 18 months; fiber law – communications capacity doubles every 9 months; and disk law – storage capability doubles every 12 months.[37] One would think, even with the pace of technology, we know most of what we need to know about computer networks. We don't. Future operations will depend on many other types of networks. While we depend upon networks our fundamental understanding of networks is primitive. In the study *Network Science*, commissioned by the Board on Army Science and Technology, researchers found "The components of modern communication and information networks are the result of technologies…emanating from physics, chemistry, and materials science. Their assembly into networks, however, is based largely on empirical knowledge rather than on a deep understanding of the principles of network behaviors gained from an underlying science of networks."[38] Physical networks are the internet, highways, air transportation networks, and global financial networks. Biological networks are our bodies metabolic and genetic expression networks. Social networks include businesses, governments, and military organizations. "The military's dependence on interacting networks in the physical, information, cognitive, and social domains is clear from its effort to transform itself into a force capable of network centric operations (NCO)."[39] But there is a gap between the military vision of NCO and our current knowledge of networks, in particular the impact of biological and social networks on physical networks. How do you standardize the current education and training when the environment in question is constantly changing?

From the previous discussions one can begin to grasp the difficulty of the IO training challenge. "The integration envisioned as not mere deconfliction, but the synchronization and harmonization of activities whose resulting effect is significantly greater than the sum of the individual components."[40] DoDi 3608.12 tasked the National Defense University to direct JFSC to develop and conduct joint IO courses. JFSC offers a one and a four week long IO courses. The objective of the Joint IO Orientation Course (JIOOC) is to educate and train personnel in the basics of joint IO, with a primary emphasis at the Combatant Command level. The focus is joint IO doctrine and DoD IO policy guidance as they apply to the operational level of joint warfare. It is relevant to those serving in support of IO cells and other staff positions that require a basic knowledge of Joint IO. The Joint Information Operations Planners Course (JIOPC) is four weeks long and establishes a common level of understanding for IO planners and IO capability specialists who will serve in joint operational-level IO billets. JIOPC does include JIOOC material and adds three weeks of intensive experience in the Joint Planning Process. It is a prerequisite for personnel assigned to the Joint IO career force.[41]

Additionally, DoDI 3608.12 tasked the Naval Postgraduate School (NPS) to establish a DoD IO Center of Excellence and to develop and maintain a graduate level program in Joint IO education. The Masters of Science in IO is 18 months in length and has been offered for two years. Graduates are taught to employ information in support of full spectrum dominance by taking advantage of information technology, exploiting the growing worldwide dependence on automated information systems, and capitalizing on near real time global dissemination of information to affect adversary decision cycles, with the goal of achieving information superiority for the U.S. This capability will be possible only after students develop a thorough understanding of the enduring nature of war. The program is "designed for both the specialist who will be assigned to an information operations position and the generalist who will be assigned to an operations directorate. The curriculum includes a core of military art and operations, the human dimension of warfare (psycho-social), analytical methods, and a technical sequence customized for each student. Additionally, each student has an elective sequence designed to further develop an in-depth understanding of joint IO."[42] But an additional confusion factor is the NPS also offers a masters degree in Information Warfare for O-3 to O-4s. The Services use this technical degree for their EW personnel. There is a significant demand for graduates from this course. The NPS IO course has not established a "demand signal" yet from the combatant commanders or services.

Based upon the complexity of the understanding required an IO warrior can't learn enough in four weeks to analyze and synthesize what they must to truly orchestrate a IO campaign.

And commanders are reluctant to release someone for 18 months to attend the limited allotment at NPS. The NPS program is treated as an Intermediate Service School and is attended by O-3's, in lieu of a masters program, or O-4 and O-5's, instead of their service school. The program is limited to 20 students, five from each service, per course. Currently the joint staff is considering whether the NPS course should be reduced to a 10-month program. Meeting a standardized set of learning objectives should set the course length not the number of days a command is willing to release a senior member for temporary duty or training.

Once an individual has IO knowledge they need train how they will fight. "Knowing is not enough; we must apply. Willing is not enough; we must do."[43] This requires application in exercises, in particular joint exercises. Currently IO is rarely used in exercises though it is becoming more common. Too often an IO capability specialist or planner's first attempt at IO is a real world situation, thrown onto a staff without the background to support him making their attempts frustrating and insufficient.

These challenges are but a few of those facing the IO career force. DoD and the Joint Staff have given the services a new IO vector. This direction is driven by the information age and the systems and speed at which we can now process information. This speed is transitioning the world out of the information age to a conceptual age. Society is moving from knowledge workers to creators and empathizers. Affluence, technology, and globalization are enabling this transition.[44] The following recommendations are offered to address these challenges and indicate those the community is currently researching or could readily implement.

Recommendations

Education and Training

Education and training require several improvements. First, there must be an executive agent for joint IO training. With the release of DoDI 3608.12, USSTRATCOM is now the operational advocate for Joint IO education. This is one of several new missions USSTRATCOM has been given. USSTRATCOM is working with the Joint Staff to standardize IO inputs for the universal joint task list and mission essential task list to accompany USSTRATCOM new IO mission. USSTRATCOM must be given the funding to support this new mission. Vision without funding is a hallucination.

IO education and training must be standardized DoD-wide and it must be adaptable enough to flow with the changes. This requires an extended review of all current IO-related education, and skill training for both IO capability specialists and planners. A joint IO training analysis is necessary to develop an effective education and training program.[45] "Desired learning objectives need to be standardized…for creating effective and comprehensive IO education and training."[46] Redundant courses must be consolidated. And those courses remaining should be jointly utilized to establish a solid IO foundation across all the Services.

A single entry level joint IO technical school used by all the Services, similar to the EW school at Pensacola, would increase standardization of knowledge across the services immediately. This course of instruction could be followed by a Service specific school to teach Service specific IO education.

IO training needs to be increased or included in all Service PME as well as leadership development courses. IO must also teach the commanders and leaders of the DoD to effectively integrate IO and IO warriors into their organization at all levels.

All IO courses must teach and strive to improve joint IO tools and software. A common set of IO tools used DoD-wide would allow an IO warrior to merge into an IO cell in any theater with only area specific spin up; thereby increasing the IO capability and ultimately the combat capability of the respective joint command.

IO must be provided a learning environment in live exercises, command post exercises, and simulations. These Joint exercises must involve full spectrum IO in the planning stage, all phases of the exercise execution and through the after action report.

Create a joint IO opposing force (OPFOR). No enemy is static. Realism in exercises requires an adversary who responds or anticipates and prepares a counter-thrust, an IO *coup fourré*.[47] A joint IO OPFOR capability, fully trained, educated, scalable, and responsive, complete with all necessary privileges to incorporate all five core capabilities in a synergistic effect could provide a realistic threat representation across a full spectrum of military operations.[48]

These education and training recommendations maximizes limited funds and facilities, and increases standardization of knowledge and application. Standardization is "essential to integrating IO TTPs into joint exercises and improving real-world IO performance."[49] As mentioned earlier, true understanding comes from application of knowledge.

Officer Accession

The IO planner career field should be a direct accession. While, IO capability specialists are initial accessions in certain functional areas. IO planners tend currently spend the early part of their career in another primary career field. Some may come from EW, PSYOP, or CNO backgrounds but currently that is the exception rather than the norm. The complexity of the environment and the knowledge required by an IO warrior requires a direct accession into an IO career field. A career broadening assignment into a "combat arms" field should be part of the career progression, not the other way around.

Use IO planners in those positions where they make the most impact. This requires identification of critical joint, Service, and combatant command IO positions. This is extremely important in the growth of the career force and in spreading the IO culture across the DoD. The BOA working group is staffing an action to accomplish just such a task.

Advocacy

Establish senior leader advocacy. The DoD is starting to see O-6 and O-7 advocacy at the joint and combatant command level. This is a great start. True advocacy, and thereby funding, must come from a senior FO/GO advocate at the Service level. The Services control the major portion of the DoD budget. Without three and four star support IO will limp along through the diligent efforts of iron majors at the operational and tactical level but languish at the strategic level. Strategic direction and advocacy is required for IO to improve and ease access. Since their creation just last year, the BoA is making strong forward progress. Identifying joint IO billets and the education requirements for the respective billets is next on the BoA activities.

The final recommendation is ironic. Use IO to improve IO. Current IO personnel don't use IO to promote or advance IO. In fact to a certain extent IO is its own worse enemy. Many IO programs are compartmentalized and even basic IO documents are close held limiting visibility to the core of the military. Without at least some visibility into the IO world why would a new officer want to be an IO warrior?

Conclusion

The DoD is moving in the right direction. The direction and doctrine provided in the latest documents have laid the foundation for a bright IO future. To realize that future requires hard work, general officer advocacy, standardization of IO training, education, and tools, and using IO to get the IO message out. The Services must align and support joint IO to defeat the existing resistance to IO as a core military competency. Without these improvements IO will continue to have "potentially marked differences in the knowledge and skill level of IO personnel from mission to mission and organization to organization."[50] These differences can be overcome but this requires guidance from senior leadership. The Board of Advisers is the best avenue to establish joint IO requirements and direction. By bringing Service IO together and aligning strong IO technical backgrounds with the other soft power IO capabilities, the DoD will develop joint IO warriors capable of executing IO as a core military competency and ensuring U.S. information dominance.

Endnotes

[1] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press ,1963), 77.

[2] Hebert, Adam J., "Information Battleground," *Air Force Magazine* , Vol. 88, No. 12 (December 2005); available from http://www.afa.org/magazine/Dec2005/1205info.html; Internet; accessed 25 Feb 2006.

[3] Under Secretary of Defense for Intelligence, "Information Operations Career Force", DoDI 3608.11 (Washington, D.C., Department of Defense, 4 Nov 2005), 1.

[4] Stephen R.Covey, *The 7 Habits of Highly Effective People* , (New York: Fireside, 1989), 97.

[5] DoDI 3608.11, 2.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] Under Secretary of Defense for Intelligence, "Joint Information Operations (IO) Education," DoDI 3608.12 (Washington, D.C., Department of Defense, 4 Nov 2005), 3-6.

[10] Director, Joint Staff, *Information Operations*, Joint Publication 3-13 (Washington, D.C. Joint Staff. February 2006), GL-9.

[11] Ibid., x.

[12] Ibid., iii.

[13] Ibid., ix.

[14] Ibid., I-1.

[15] Ibid.

[16] Ibid., I-2.

[17] Ibid., I-9.

[18] Ibid., II-2

[19] Ibid.

[20] Ibid., II-4.

[21] Ibid., II-5.

[22] U.S. Department of the Army, *Commissioned Officer Professional Development and Career Management*, Army Pamphlet 600-3 (Washington, D.C.: U.S. Department of the Army 600-3, 28 December2005), 227; available from http://www.apd.army.mil/pdffiles/p600_3.pdf; Internet; accessed 13 April 2006.

[23] HQ AFDC/DR, *Information Operations*, AFDD 2-5 (Washington D.C., HQ USAF, 11 Jan 05), 5.

[24] Mr. Paul Scott, Air Combat Command A3I, telephone interview by author, 24 February and 6 April 2006. Scientists is a mix of computer scientists, physicists, and mathematicians.

[25] CAPT Stephanie Helm, N3IO, IO Branch Chief, telephone interview by author and e-mail, 13 April 2006.

[26] This concept was first published in an article by Edward Hanlon, Jr., LtGen, USMC, "A Concept for Information Operations," (Quantico, Marine Corps Combat Development Command, 19 Apr 2002), 1 and then revised and slightly updated in the *Marine Corps' Concepts and Programs Document,* (Washington D.C., HQ USMC, 2006) 39. The latest version is used.

[27] HQ USMC, *Marine Occupational Specialties Manual* , MCO P1200.16, (Washington D.C., HQ USMC, 18 April 2005), 1- 108, 1-144.

[28] Col J. R. Wassink, HQ USMC, Branch Chief PLI, telephone interview by author and e-mails, 6 -11 April 2006.

[29] Secretary of Defense, Quadrennial Defense Review Report, (Washington D.C., Office of the Secretary of Dense, 6 Feb 2006), 92.

[30] JP 3-13, VII-1.

[31] Ibid.

[32] Ibid., VII-2.

[33] Information Assurance Technology Analysis Center (IATAC), *The Joint Information Operations Integrated Training and Exercise Roadmap & Investment Strategy* (Falls Church: IATAC – Booze Allen), 20.

[34] JP 3-13, VII-2.

[35] Ibid.

[36] Ibid.

[37] Al Shaffer, "Transitioning S&T Programs" briefing slides presented to the Defense Systems Acquisition Management Course, 17 June 2004; available from http://proceedings.ndia.org/402C/402C_Shaffer.pdf; Internet, accessed 7 Apr 2006.

[38] The National Academy of Science, *Network Science*, (Washington D.C.: The National Academy Press, 2005), 26.

[39] Ibid., 1.

[40] COL David J. Smith, ed., *Information Operations Primer*, (Carlisle Barracks, PA: U.S. Army War College, January 2006), 1.

[41] *The Information Operations Division Home Page*, available from http://www.jfsc.ndu.edu/schools_programs/jc2ios/io/default.asp; Internet; accessed 7 April 2006.

[42] The Graduate School of Operations and Information Sciences Home Page, available from http://www.nps.navy.mil/GSOIS/programs/programs_009.htm ; Internet; accessed 7 April 2006.

[43] Bruce Lee, *Quoteworld*, available from http://www.quoteworld.org/quotes/8155; Internet; accessed 7 April 2006.

[44] Daniel H. Pink, *A Whole New Mind*, (New York: The Penguin Group, 2005), 49.

[45] IATAC, 53.

[46] Ibid., 32.

[47] Coup Fourré a French fencing term for counter-thrust where one fencer parries his opponent's thrust and counter attacks in the same maneuver.

[48] IATAC, 76.

[49] Ibid.

[50] Ibid., 53.